collabria

At Collabria, the security of our cardholders' information is of utmost importance, and we are committed to keeping you informed about potential risks.

Recently, we have identified several websites replicating Collabria secure sites. The most recent false websites can be identified by the ending in their domain, which ends with ".life" rather than ".ca" or ".com", such as "collabriacreditcards.life". These websites appear to be phishing sites designed to capture user information.

As your trusted credit card provider, we want to assure you that our security team is actively working to address this risk and mitigate any potential harm to our cardholders. This email is to provide you with as much information as possible to safeguard your information.

- Only access the official websites and applications when managing your credit card accounts or submitting a card application and avoid clicking on links from unknown sources, including search engine results. The following are the only official Collabria websites and applications:
    - www.collabriafinancial.ca
    - https://www.collabriacreditcards.ca
    - https://www.cardwiseonline.ca
    - https://www.mycardinfo.com
- Always exercise caution when providing your personal information or credit card details online.
- Regularly review your credit card transactions for any suspicious activity and promptly report any unauthorized transactions to Collabria's Cardholder Services. The telephone number is readily available on the back of your physical card.
- As good practice, access platform links from trusted sources. For example, your credit union may have a trusted link to platforms designed to digitally access your credit card account. Once you have accessed the trusted location, add it to your bookmarks.

- The CardWise digital account management platform is also available to you as a mobile application, accessible from your mobile device. CardWise Mobile can be downloaded from your phone’s app store. As manner of design, mobile applications have many built-in security features, such as biometric login, and are not easily replicated.
- When accessing a website, please proceed with caution if you’re asked to download an application. Collabria will not ask you to download any applications to your desktop computer directly from a website.
- We appreciate your cooperation and support in maintaining the security of your information. Rest assured that we are fully committed to protecting you and your credit union from any potential threats.

Thank you for your attention to this matter.
Sincerely,

Collabria Financial Services

FAQ

Q1: What should I do if I suspect I have provided my personal information to a phishing website?

A1: If you believe you have provided your personal information to a phishing website, immediately contact Collabria's Cardholder Services using the telephone number on the back of your physical card. Our team will guide you through the necessary steps to secure your account and prevent any unauthorized transactions.

Q2: How can I identify a legitimate Collabria website or application?

A2: Legitimate Collabria websites and applications have domain names ending in "ca" or "com", such as "collabriafinancial.ca" or "collabriacreditcards.ca". Always access these platforms through trusted sources, such as your credit union's website or by typing the URL directly into your browser. Avoid clicking on links from unknown sources or search engine results.

Q3: What should I do if I notice suspicious or unauthorized transactions on my credit card statement?

A3: If you notice any suspicious or unauthorized transactions on your credit

card statement, immediately report them to Collabria's Cardholder Services using the telephone number on the back of your physical card. Our team will investigate the transactions and take the necessary steps to resolve the issue and protect your account.

Q4: Is it safe to use the CardWise Mobile application?

A4: Yes, the CardWise Mobile application is a secure way to manage your credit card account. Mobile apps have built-in security features, such as biometric login, and are more difficult to replicate than websites. Always download the app from your phone's official app store to ensure you are using the legitimate application.

Q5: What measures is Collabria taking to address the risk of phishing websites?

A5: Collabria's security team is actively working to identify and mitigate the risk posed by phishing websites. We are committed to protecting our cardholders' information and are continuously monitoring for potential threats. Additionally, we are sending out communications like this one to inform and educate our cardholders about the risks and the steps they can take to protect themselves.

Q6: Who should I contact if I have more questions or concerns about the security of my credit card account?

A6: If you have any additional questions or concerns about the security of your credit card account, please don't hesitate to contact Collabria's Cardholder Services using the telephone number on the back of your physical card. Our team is available to assist you and provide the support you need to ensure the safety of your account.

Q7: Why did I receive an email about security risks?

A7: We issued a security alert to all our cardholders, including those who have opted out of marketing communications, due to the discovery of counterfeit websites mimicking Collabria's official sites. This communication is part of our commitment to your security and aims to inform you about the potential risk.

Q8: What should I avoid to prevent landing on a phishing website?

A8:

- Only click on website links from trusted sources.
- Bookmark sites that you use on a regular basis
- Avoid doing a search on your desktop search engine and clicking on sponsored ads

Q9: How can I identify a phishing website?

A9: Phishing websites often have URLs that are slightly altered from the legitimate site's URL. For example, fraudulent sites may end with ".life" instead of ".ca" or ".com". Always check the URL carefully before entering any personal information.

Q10: What should I do if I suspect I've visited a phishing site?

A10: If you suspect you've entered personal information on a phishing site, immediately change your account passwords and monitor your account for any suspicious activity.

Q11: How can I protect myself from phishing scams?

A11: Always verify the authenticity of a website before entering personal information. Bookmark the official Collabria websites and only use these bookmarks to access your account. Be cautious of links from unknown sources and regularly review your credit card statements for any unauthorized transactions.

Q12: Are mobile apps safer than websites?

A12: Yes, mobile apps like CardWise have additional built-in security features, such as biometric logins, making them more secure and harder to replicate by fraudsters. We recommend using our mobile app for accessing your account information.

Q13: Should I download the CardWise platform from your website?

A13: No. CardWise Online is accessible by typing the address in your internet browser. It will be available at www.cardwiseonline.ca. The CardWise Mobile application is only available from your phone’s application store. Collabria will never ask you to download an application to your desktop.

collabria